**Server Security Policy**

**1.0 Purpose**

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by ***<Company Name>.*** Effective implementation of this policy will minimize unauthorized access to ***<Company Name>*** proprietary information and technology.

**2.0 Scope**

This policy applies to server equipment owned and/or operated by ***<Company Name>***, and to servers registered under any ***<Company Name>***-owned internal network domain.

This policy is specifically for equipment on the internal ***<Company Name>*** network.

**3.0 Policy**

**3.1 Ownership and Responsibilities**

An operational group that is responsible for system administration must own all internal servers deployed at ***<Company Name>***. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by ***<Company Name>***. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment.

Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

* + Server contact(s) and location, and a backup contact
  + Hardware and Operating System/Version
  + Main functions and applications, if applicable

Information in the corporate enterprise management system must be kept up-to-date.

Configuration changes for production servers must follow the appropriate change management procedures.

**3.2 General Configuration Guidelines**

* Operating System configuration should be in accordance with approved guidelines.
* Services and applications that will not be used must be disabled where practical. Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
* The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
* Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
* Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.
* If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
* Servers should be physically located in an access-controlled environment. Servers are specifically prohibited from operating from uncontrolled cubicle areas.

**3.3 Monitoring**

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

* All security related logs will be kept online for a minimum of 1 week.
* Daily incremental tape backups will be retained for at least 1 month.
* Weekly full tape backups of logs will be retained for at least 1 month.
* Monthly full backups will be retained for a minimum of 2 years.

Security-related events will be reported to ***<Company Name>***, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

* Port-scan attacks
* Evidence of unauthorized access to privileged accounts
* Anomalous occurrences that are not related to specific applications on the host.

**3.4 Compliance**

* Audits will be performed on a regular basis by authorized organizations within ***<Company Name>.***
* Audits will be managed by the internal audit group in accordance with the *Audit Policy*. ***<Company Name>*** will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
* Every effort will be made to prevent audits from causing operational failures or disruptions.

**4.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**Source:** <http://www.cpcstech.com/pdf/server_security_policy.pdf>